目 录

1 WAPI

1.1 WAPI简介

WAPI（WLAN Authentication and Privacy Infrastructure，无线局域网鉴别与保密基础结构）是中国提出的以 802.11 无线协议为基础的无线安全标准。

WAPI 采用证书认证方式和预共享密钥认证方式对客户端身份的合法性进行认证，并且采用单播密钥协商和组播密钥通告对客户端和与 AC 之间交互的单播/组播数据进行保护。

1.1.1 WAPI 协议的构成

WAPI 协议由以下两部分构成：

- WAI（WLAN Authentication Infrastructure，无线局域网鉴别基础结构）：用于无线局域网中身份认证和密钥管理的安全方案。
- WPI（WLAN Privacy Infrastructure，无线局域网保密基础结构）：用于无线局域网中数据传输保护的安全方案，包括数据加解密和重放保护等功能。

1.1.2 基本概念

- AS（Authentication Server，认证服务器）：用于对用户和设备证书进行身份认证等，是基于公钥密码技术的 WAI 中重要的组成部分。
- BK（Base Key，基密钥）：用于导出单播会话密钥，由证书认证过程协商得到或者由预共享密钥导出。
- MSK（Multicast Session Key，组播会话密钥）：用于保护站点发送的组播 MPDU 的随机值，包括组播加密密钥和组播完整性校验密钥。
- PSK（Preshared Key，预共享密钥）：发布给客户端的静态密钥。
- USK（Unicast Session Key，单播会话密钥）：由 BK 通过伪随机函数导出的随机值，分为四个部分：单播加密密钥、单播完整性校验密钥、消息认证密钥和组播密钥加密密钥。

1.1.3 WAPI 的身份认证方式

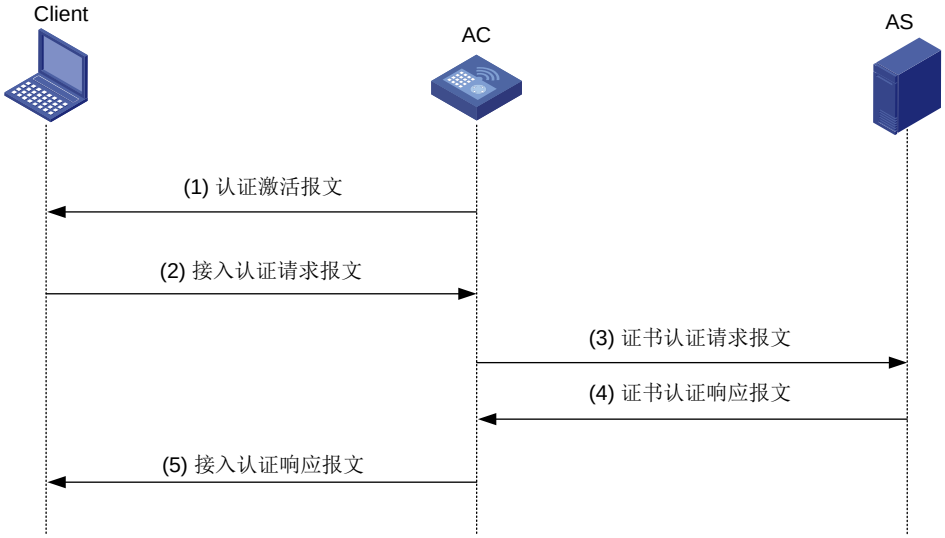
WAPI 支持两种身份认证方式：证书认证方式和预共享密钥认证方式。

1. 证书认证方式

证书认证是基于无线客户端、AC 和 AS 三方的证书进行的认证。认证前无线客户端和 AC 必须预先拥有各自的证书，然后通过 AS 对双方的身份分别进行认证，根据双方产生的临时公钥和临时私钥生成 BK，并为随后的单播密钥协商和组播密钥通告做好准备。有关证书认证的详细介绍，请参见“安全配置指导”中的“PKI”。

目前，AC 与 AS 之间的 WAI 协议报文将通过普通的 UDP 方式进行传输，最终完成证书认证，具体过程如图 1-1 所示。

图1-1 证书认证过程



(1) 802.11 链路协商完成以后，AC 会向 Client 发送认证激活报文启动证书认证过程，其中包含 AC 的证书。

(2) Client 接收到认证激活报文后，向 AC 发送接入认证请求报文，其中包含 Client 证书及 Client 对接入认证请求报文的签名。

(3) AC 接收到接入认证请求报文后，从 Client 证书中取出公钥，验证签名是否正确，如果签名正确，则向 AS 发送证书认证请求报文，其中包含 Client 证书和 AC 证书，如果签名不正确，则丢弃报文。

(4) AS 收到证书认证请求报文后，验证 Client 证书和 AC 证书是否正确，并向 AC 发送证书认证响应报文，其中包含验证结果和 AS 签名。

(5) AC 收到证书认证响应报文后，向 Client 发送接入认证响应报文，其中包含接入认证结果，证书验证结果，AS 签名，AC 对接入认证响应报文的签名。

(6) Client 收到接入认证响应报文后，依次检查 AC 的证书验证结果和接入认证结果：

a. 如果 AC 证书不正确，则断开连接；如果正确，检查接入认证结果。

b. 如果结果为接入成功，则进行单播密钥协商和组播密钥通告，否则断开连接。

2. 预共享密钥认证方式

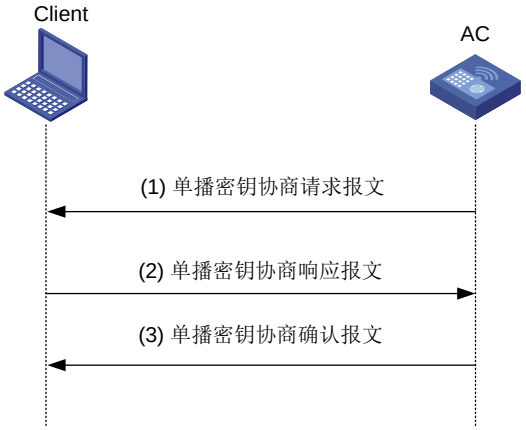
预共享密钥认证是基于 Client 和 AC 双方的密钥所进行的认证。认证前 Client 和 AC 必须预先配置有相同的密钥，即预共享密钥。认证时直接将预共享密钥转换为 BK，然后进行单播密钥协商和组播密钥通告。

1.1.4 WAPI 的密钥管理

1. 单播密钥协商

Client 与 AC 之间交互的单播数据利用单播密钥协商过程所协商出的单播加密密钥和单播完整性校验密钥进行保护，其过程如图 1-2 所示。

图1-2 单播密钥协商过程



(1) 在 AC 完成证书认证过程、采用预共享密钥认证方式或进行单播密钥更新时，AC 向 Client 发送单播密钥协商请求报文开始与 Client 进行单播密钥协商，其中包含 AC 的 Challenge 字段。

(2) Client 接收到 AC 发送的单播密钥协商请求报文后：

- 如果是 Client 上线过程，则直接发送单播密钥协商响应报文。
- 如果是单播密钥更新过程，会检查 AC 的 Challenge 字段与本地保存的值是否相同，此时本地保存的值为上一次协商的值，如果相同，则发送单播密钥协商响应报文，否则丢弃报文。

单播密钥协商响应报文中包含 Client 的 Challenge 字段、AC 的 Challenge 字段以及消息认证码。

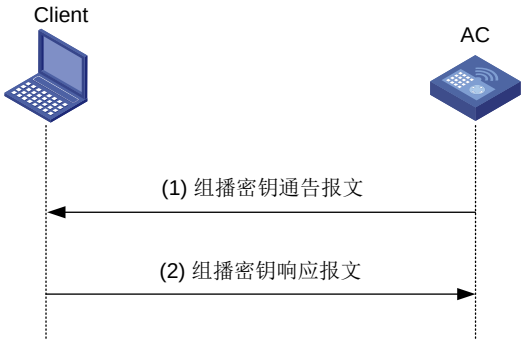
(3) AC 接收到单播密钥协商响应报文后，验证 AC 的 Challenge 字段和消息认证码是否正确，如果正确，则发送单播密钥协商确认报文，其中包含 Client 的 Challenge 字段和消息认证码，如果不正确则丢弃报文。

(4) Client 接收到单播密钥协商确认报文后，验证 Client 的 Challenge 字段和消息认证码是否正确，如果正确则协商完成，如果不正确则丢弃报文。

2. 组播密钥通告

当单播密钥协商完成后，再使用单播密钥协商过程所协商出的密钥进行组播密钥的通告。AC 利用自己生成的 16 个字节的随机数(只生成一次)，即组播密钥对其发送的广播/组播数据进行保护，而 Client 则采用 AC 通告的组播会话密钥对收到的广播/组播数据进行解密。其过程如图 1-3 所示。

图1-3 组播密钥通告过程



(1) 单播密钥协商成功后或 AC 要更新组播密钥时，AC 向 Client 发送组播密钥通告报文，包含密钥数据、密钥通告标识等。

(2) Client 接收到 AC 发送的组播密钥通告报文后，对密钥数据解密得到通告主密钥，然后向 AC 发送组播密钥响应报文，其中包含密钥通告标识。

(3) AC 接收到 Client 发送的组播密钥响应报文后，验证密钥通告标识是否正确，如果正确则组播密钥通告成功，如果不正确则丢弃报文。

1.1.5 协议规范

与 WAPI 相关的协议规范有：

- GB 15629.11-2003/XG1-2006：信息技术系统间远程通信和信息交换局域网和城域网 特定要求 第 11 部分：无线局域网媒体访问控制和物理层规范
- RFC 3280：Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 4492：Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

产品系列	产品型号	说明
WX2500H-WiNet系列	WX2510H-PWR-WiNet WX2560H-WiNet	支持
WX3500H-WiNet系列	WX3508H-WiNet	支持
WAC系列	WAC380-30 WAC380-60 WAC380-90 WAC380-120 WAC381	WAC380-30支持 WAC380-60支持 WAC380-90支持 WAC380-120支持 WAC381不支持
WX2500H-LI系列	WX2540H-LI WX2560H-LI	支持
WX3500H-LI系列	WX3510H-LI WX3520H-LI	支持

1.2 WAPI配置限制和指导

请在配置本功能之前通过 **a-msdu disable** 命令关闭 A-MSDU 功能。有关 A-MSDU 功能的详细介绍请参见“射频资源管理配置指导”中的“射频管理”。

WAPI 协议规定在证书认证过程中所使用的密钥签名算法必须为 ECDSA（Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法），有关 ECDSA 的详细介绍，请参见“安全配置指导”中的“公钥管理”。

WAPI 仅支持数据集中转发方式，不支持数据本地转发方式。

Dot11ac 模式下，不建议配置本特性。

1.3 WAPI配置任务简介

WAPI 配置任务如下：

(1) 配置 WAPI 认证方式

(2) 配置 WAPI 采用证书认证

如果选择的 WAPI 认证方式包括证书认证，则需要进行此配置。

(3) 配置 WAPI 采用预共享密钥认证

如果选择的 WAPI 认证方式包括预共享密钥认证，则需要进行此配置。

(4) 开启 WAPI 认证功能

(5) 配置 WAPI 用户使用指定的 ISP 域进行 AAA 认证

如果 WAPI 用户需要计费，则需要进行此配置。

(6) 配置单播密钥更新

(7) 配置组播密钥更新

1.4 配置WAPI认证方式

(1) 进入系统视图。

system-view

(2) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 配置 WAPI 认证方式。

wapi authentication-method { **certificate** | **certificate-or-psk** | **psk** }

缺省情况下，WAPI 采用证书认证方式。

1.5 配置WAPI采用证书认证

WAPI 采用证书认证的配置任务如下：

(1) 配置认证服务器的 IP 地址

(2) 配置证书所属的 PKI 域和证书序列号

(3) （可选）配置基密钥更新功能

1.5.2 配置认证服务器的 IP 地址

1. 功能简介

当 WAPI 采用证书认证方式时，设备会与认证服务器交互验证证书。

2. 配置限制和指导

一个无线服务模板下只能配置一个认证服务器的 IP 地址。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 配置认证服务器的 IP 地址。

wapi authentication-server ip *ip-address*

缺省情况下，未配置认证服务器的 IP 地址。

1.5.3 配置证书所属的 PKI 域和证书序列号

1. 功能简介

指定证书所属的 PKI 域，用于获取对应 PKI 域的相关策略；指定证书序列号，用于查找和获取认证服务器上的证书。

2. 配置限制和指导

一个无线服务模板下只能配置一个 PKI 域和证书序列号。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 配置证书所属的 PKI 域和证书序列号。

wapi certificate domain *domain-name* **serial** *serial-number*

缺省情况下，未配置证书所属的 PKI 域和证书序列号。

1.5.4 配置基密钥更新功能

1. 功能简介

基密钥具有生命周期，当其生命周期结束时需要进行更新。

2. 配置限制和指导

要进行基密钥更新，必须保证基密钥更新功能处于开启状态。

在单播密钥更新功能处于开启状态时，基密钥更新完成后，单播密钥也会进行更新，而不受单播密钥生存周期的影响，当单播密钥更新完成后基密钥才会重新开始计算生存周期。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 开启基密钥更新功能。

wapi bk-rekey enable

缺省情况下，基密钥更新功能处于开启状态。

(4) 配置基密钥生存周期。

wapi bk lifetime *time*

缺省情况下，基密钥生存周期为 43200 秒。

1.6 配置WAPI采用预共享密钥认证

(1) 进入系统视图。

system-view

(2) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 配置 WAPI 预共享密钥。

wapi psk { **cipher** | **simple** } { **hex** | **string** } *key*

缺省情况下，未配置 WAPI 预共享密钥。

1.7 开启WAPI认证功能

1. 配置准备

请在开启 WAPI 认证功能前，先关闭无线服务模板。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 开启 WAPI 认证功能。

wapi enable

缺省情况下，WAPI 认证功能处于关闭状态。

1.8 配置WAPI用户使用指定的ISP域进行AAA认证

1. 功能简介

WAPI 用户将采用指定的 ISP 域内的计费方案对 WAPI 用户进行计费。

2. 配置限制和指导

请先通过 **domain** 命令创建 ISP 域，然后再通过本命令引用创建的 ISP 域，关于 **domain** 命令的详细介绍，请参见“用户接入与认证命令参考”中的“AAA”。

目前，当 ISP 域里面配置了认证、授权和计费方案后，仅计费方案生效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 配置 WAPI 用户使用指定的 ISP 域进行 AAA 认证。

wapi domain *domain-name*

缺省情况下，未配置 WAPI 用户使用的 ISP 域，即不对用户进行 AAA 认证。

1.9 配置单播密钥更新

1. 功能简介

单播密钥具有生命周期，开启单播密钥更新功能后，单播密钥在其生命周期结束后会自动进行更新。

2. 配置限制和指导

要进行单播密钥更新，必须保证单播密钥更新功能处于开启状态。

在单播密钥更新功能处于开启状态时，基密钥更新完成后，单播密钥也会进行更新，而不受单播密钥生存周期的影响。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 开启单播密钥更新功能。

wapi usk-rekey enable

缺省情况下，单播密钥更新功能处于开启状态。

(4) 配置单播密钥的生存周期。

wapi usk lifetime *time*

缺省情况下，单播密钥的生存周期为 86400 秒。

1.10 配置组播密钥更新

1. 功能简介

组播密钥具有生命周期，当其生命周期结束时需要更新组播密钥。组播密钥更新支持以下方式：

- 由流量触发组播密钥更新。
- 定期触发组播密钥更新。

2. 配置限制和指导

为了保证用户下线触发组播密钥更新功能生效，请保证首先开启了组播密钥更新功能。

由流量触发组播密钥更新和定期触发组播密钥更新不能同时配置。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 开启组播密钥更新功能。

wapi msk-rekey enable

缺省情况下，组播密钥更新功能处于开启状态。

(4) 开启用户下线触发组播密钥更新功能。

wapi msk-rekey client-offline enable

缺省情况下，用户下线触发组播密钥更新功能处于关闭状态。

(5) 配置组播密钥更新触发方式。

wapi msk-rekey method { **packet-based** [**packet**] | **time-based** [*interval*] }

缺省情况下，组播密钥更新触发方式为定期方式。

1.11 WAPI显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 WAPI 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 WAPI 的统计信息。

表1-1 WAPI 显示和维护

操作	命令
显示WAPI的统计信息	**display wapi statistics** [**ap** *ap-name* [**radio** *radio-id*]]
显示WAPI用户的信息	**display wapi user** [**ap** *ap-name* [**radio** *radio-id*] | **user-mac** *mac-address*]
清除WAPI的统计信息	**reset wapi statistics** [**ap** *ap-name* [**radio** *radio-id*]]

1.12 WAPI典型配置举例

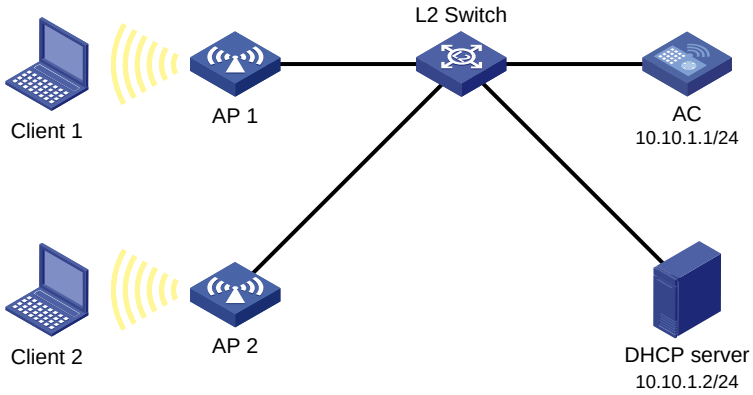
1.12.1 预共享密钥认证配置举例

1. 组网需求

- AP 1 和 AP 2 通过二层交换机与 AC 建立连接，Client 1 和 Client 2 分别通过 AP 1 和 AP 2 接入网络。
- Client 1、Client 2、AP 1 和 AP 2 都从 DHCP 服务器获取 IP 地址。
- Client 采用预共享密钥认证方式接入，Client 端和 AC 端使用相同的共享密钥 12345678；单播密钥和组播密钥的更新时间均为 20000 秒。

2. 组网图

图1-4 预共享密钥认证配置组网图



3. 配置步骤

(1) 配置 IP 地址

请按照图 1-4 配置各设备的 IP 地址和子网掩码，具体配置过程略。

(2) 配置 AC

创建无线服务模板 1，SSID 为 wapi1。

```
[AC] wlan service-template 1
[AC-wlan-st-1] ssid wapi1
```

开启 WAPI 认证功能。

```
[AC-wlan-st-1] wapi enable
```

配置 WAPI 采用预共享密钥认证方式。

```
[AC-wlan-st-1] wapi authentication-method psk
[AC-wlan-st-1] wapi psk simple string 12345678
[AC-wlan-st-1] wapi msk-rekey method time-based 20000
[AC-wlan-st-1] wapi usk lifetime 20000
[AC-wlan-st-1] service-template enable
```

创建型号为 WA3628i-AGN 的 AP 管理模板 ap1，并配置其序列号为 210235A29G007C000020。

```
[AC] wlan ap ap1 model WA3628i-AGN
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

创建射频 1，配置其与无线服务模板 1 关联，并开启该射频。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

创建型号为 WA3628i-AGN 的 AP 管理模板 ap2，并配置其序列号为 210235A29G007C000021。

```
[AC] wlan ap ap2 model WA3628i-AGN
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

创建射频 1，配置其与无线服务模板 1 关联，并开启该射频。

```
[AC-wlan-ap-ap2] radio 1
[AC-wlan-ap-ap2-radio-1] service-template 1
[AC-wlan-ap-ap2-radio-1] radio enable
[AC-wlan-ap-ap2-radio-1] quit
[AC-wlan-ap-ap2] quit
```

4. 验证配置

通过使用 **display wapi user** 命令可以查看接口上 WAPI 用户的信息。例如：

查看 AC 所有接口上 WAPI 用户的信息。

```
[AC] display wapi user
Total number of users: 2

AP name                                 : ap1
Radio ID                                : 1
SSID                                    : wapi1
BSSID                                   : 487a-da52-d4f0
MAC address                             : 000b-c002-5e39
VLAN                                    : 1
Authentication method                   : PSK
Current state                           : Online
    Authentication state                : Idle
    Unicast key negotiation state       : Established
    Multicast key negotiation state     : Established
    Authorization state                 : Idle
    Accounting state                    : Idle
Uptime                                  : 00:02:26

AP name                                 : ap1
Radio ID                                : 1
SSID                                    : wapi1
BSSID                                   : 487a-da52-d4f0
MAC address                             : 000b-c002-5e2f
VLAN                                    : 1
Authentication method                   : PSK
Current state                           : Online
    Authentication state                : Idle
```

```
    Unicast key negotiation state          : Established
    Multicast key negotiation state        : Established
    Authorization state                    : Idle
    Accounting state                       : Idle
Uptime                                     : 00:02:40
```

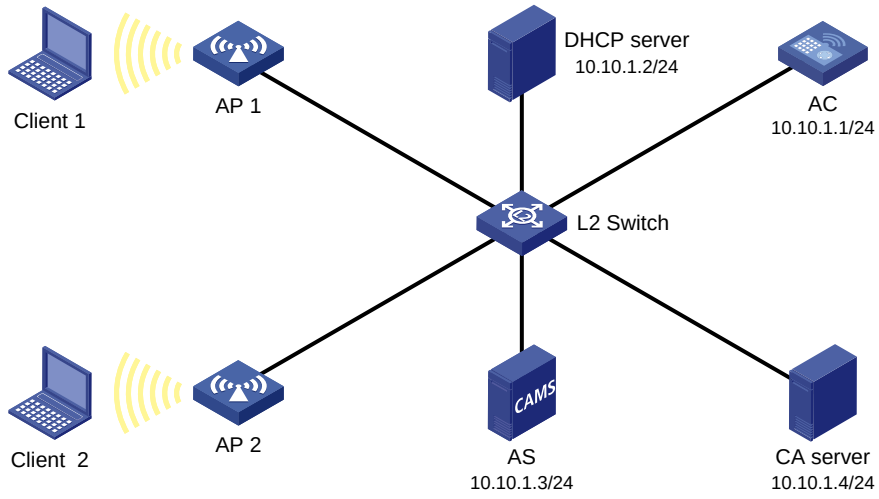
1.12.2 标准证书认证配置举例

1. 组网需求

- AP 1 和 AP 2 通过二层交换机与 AC 建立连接，Client 1 和 Client 2 分别通过 AP 1 和 AP 2 接入网络。
- Client 1、Client 2、AP 1 和 AP 2 都从 DHCP 服务器获取 IP 地址。
- CA 证书、AC 本地证书和 AS 证书均已保存至 AC；单播密钥和组播密钥的更新时间均为 20000 秒，关闭 BK 更新功能。

2. 组网图

图1-5 标准证书认证配置组网图



说明

- AS 和 CA 服务器可以是同一台物理设备，这种情况下，AS 证书和 CA 证书是一个证书。
- AS 上需要依次导入 CA 证书和 AS 证书。WAPI 客户端上需要安装 asue 证书和 AS 证书。

3. 配置步骤

(1) 配置 IP 地址

请按照图 1-5 配置各设备的 IP 地址和子网掩码，具体配置过程略。

(2) 配置 AC

创建 PKI 域 pki1，在该域中禁止 CRL 检查（对导入的证书不进行是否吊销检查，即默认此方式下用户证书有效）。

```
<AC> system-view
```

```
[AC] pki domain pki1
[AC-pki-domain-pki1] undo crl check enable
[AC-pki-domain-pki1] quit
```

分别导入证书文件 ca.cer、ap.cer 和 as.cer。

```
[AC] pki import domain pki1 pem ca filename ca.cer
[AC] pki import domain pki1 pem local filename ap.cer
[AC] pki import domain pki1 pem peer filename as.cer
```

创建服务模板 1，配置其 SSID 为 wapi1。

```
[AC] wlan service-template 1
[AC-wlan-st-1] ssid wapi1
```

开启 WAPI 认证功能。

```
[AC-wlan-st-1] wapi enable
```

配置 WAPI 采用证书认证方式。

```
[AC-wlan-st-1] wapi authentication-method certificate
[AC-wlan-st-1] wapi authentication-server ip 10.10.1.3
[AC-wlan-st-1] wapi certificate domain pki1 serial 29
[AC-wlan-st-1] undo wapi bk-rekey enable
[AC-wlan-st-1] wapi msk-rekey method time-based 20000
[AC-wlan-st-1] wapi usk lifetime 20000
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

创建型号为 WA3628i-AGN 的 AP 管理模板 ap1，并配置其序列号为 210235A29G007C000020。

```
[AC] wlan ap ap1 model WA3628i-AGN
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

创建射频 1，配置其与无线服务模板 1 关联，并开启该射频。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

创建型号为 WA3628i-AGN 的 AP 管理模板 ap2，并配置其序列号为 210235A29G007C000021。

```
[AC] wlan ap ap2 model WA3628i-AGN
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

创建射频 1，配置其与无线服务模板 1 关联，并开启该射频。

```
[AC-wlan-ap-ap2] radio 1
[AC-wlan-ap-ap2-radio-1] service-template 1
[AC-wlan-ap-ap2-radio-1] radio enable
[AC-wlan-ap-ap2-radio-1] quit
[AC-wlan-ap-ap2] quit
```

4. 验证配置

通过使用 **display wapi user** 命令可以查看接口上 WAPI 用户的信息。例如：

查看 AC 所有接口上 WAPI 用户的信息。

```
[AC] display wapi user
```

```
Total number of users: 2

AP name                                  : ap1
Radio ID                                 : 1
SSID                                     : wapi1
BSSID                                    : 487a-da52-d4f0
MAC address                              : 000b-c002-5e39
VLAN                                     : 1
Authentication method                    : Certificate
Current state                            : Online
    Authentication state                 : Authenticated
    Unicast key negotiation state        : Established
    Multicast key negotiation state      : Established
    Authorization state                  : Idle
    Accounting state                     : Idle
Uptime                                   : 00:02:26

AP name                                  : ap1
Radio ID                                 : 1
SSID                                     : wapi1
BSSID                                    : 487a-da52-d4f0
MAC address                              : 000b-c002-5e2f
VLAN                                     : 1
Authentication method                    : Certificate
Current state                            : Online
    Authentication state                 : Authenticated
    Unicast key negotiation state        : Established
    Multicast key negotiation state      : Established
    Authorization state                  : Idle
    Accounting state                     : Idle
Uptime                                   : 00:02:30
```

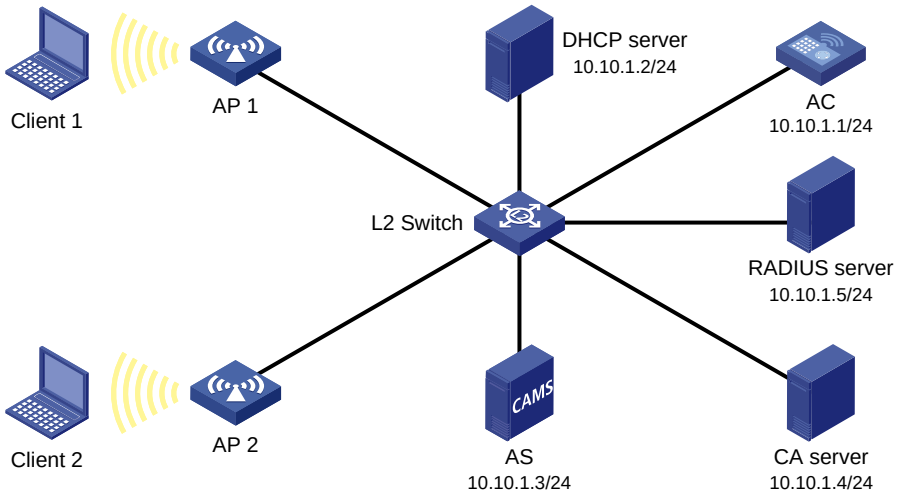
1.12.3 标准证书认证进行计费配置举例

1. 组网需求

- AP 1 和 AP 2 通过二层交换机与 AC 建立连接，Client 1 和 Client 2 分别通过 AP 1 和 AP 2 接入网络。
- Client 1、Client 2、AP 1 和 AP 2 都从 DHCP 服务器获取 IP 地址。
- WAPI 系统采用证书认证方式中的标准证书认证模式，CA 证书、AC 本地证书和 AS 证书均已保存至 AC；单播密钥和组播密钥的更新时间均为 20000 秒，关闭 BK 更新功能。
- 对用户进行计费。

2. 组网图

图1-6 证书认证进行计费配置组网图



说明

- AS、CA 服务器和 RADIUS 服务器可以是同一台物理设备，这种情况下，AS 证书和 CA 证书是一个证书。
- AS 上需要依次导入 CA 证书和 AS 证书。WAPI 客户端上需要安装 asue 证书和 AS 证书。

3. 配置步骤

(1) 配置 IP 地址

请按照图 1-6 配置各设备的 IP 地址和子网掩码，具体配置过程略。

(2) 配置 AC

创建 PKI 域 pki1，在该域中禁止 CRL 检查（对导入的证书不进行是否吊销检查，即默认此方式下用户证书有效）。

```
<AC> system-view
[AC] pki domain pki1
[AC-pki-domain-pki1] undo crl check enable
[AC-pki-domain-pki1] quit
```

分别导入证书文件 ca.cer、ap.cer 和 as.cer。

```
[AC] pki import domain pki1 pem ca filename ca.cer
[AC] pki import domain pki1 pem local filename ap.cer
[AC] pki import domain pki1 pem peer filename as.cer
```

创建 RADIUS 方案 radius1，主认证/授权服务器和主计费服务器的 IP 地址均为 10.10.1.5，RADIUS 认证/授权报文和计费报文的共享密钥均为 12345678。

```
[AC] radius scheme radius1
[AC-radius-radius1] primary authentication 10.10.1.5
[AC-radius-radius1] primary accounting 10.10.1.5
[AC-radius-radius1] key authentication simple 12345678
[AC-radius-radius1] key accounting simple 12345678
[AC-radius-radius1] quit
```

创建 ISP 域 domain1，将 WAPI 用户的认证、授权方案配置成 none，计费方案配置为 radius1，并将该域配置为缺省 ISP 域。

```
[AC] domain domain1
[AC-isp-domain1] authentication default none
[AC-isp-domain1] authorization default none
[AC-isp-domain1] accounting default radius-scheme radius1
[AC-isp-domain1] quit
[AC] domain default enable domain1
```

创建服务模板 1，配置其 SSID 为 wapi1。

```
[AC] wlan service-template 1
[AC-wlan-st-1] ssid wapi1
```

开启 WAPI 认证功能。

```
[AC-wlan-st-1] wapi enable
```

配置 WAPI 采用证书认证方式。

```
[AC-wlan-st-1] wapi authentication-method certificate
[AC-wlan-st-1] wapi authentication-server ip 10.10.1.3
[AC-wlan-st-1] wapi certificate domain pki1 serial 29
[AC-wlan-st-1] wapi domain domain1
[AC-wlan-st-1] undo wapi bk-rekey enable
[AC-wlan-st-1] wapi msk-rekey method time-based 20000
[AC-wlan-st-1] wapi usk lifetime 20000
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

创建型号为 WA3628i-AGN 的 AP 管理模板 ap1，并配置其序列号为 210235A29G007C000020。

```
[AC] wlan ap ap1 model WA3628i-AGN
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

创建类型为 802.11b 的射频 1，配置其与服务模板 1 关联，并使能该射频。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

创建型号为 WA3628i-AGN 的 AP 管理模板 ap2，并配置其序列号为 210235A29G007C000021。

```
[AC] wlan ap ap2 model WA3628i-AGN
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

创建类型为 802.11b 的射频 1，配置其与无线服务模板 1 关联，并开启该射频。

```
[AC-wlan-ap-ap2] radio 1
[AC-wlan-ap-ap2-radio-1] service-template 1
[AC-wlan-ap-ap2-radio-1] radio enable
[AC-wlan-ap-ap2-radio-1] quit
[AC-wlan-ap-ap2] quit
```

4. 验证配置

通过使用 **display wapi user** 命令可以查看接口上 WAPI 用户的信息。例如：

查看 AC 所有接口上 WAPI 用户的信息。

```
[AC] display wapi user
Total number of users: 2

AP name                                 : ap1
Radio ID                                : 1
SSID                                    : wapi1
BSSID                                   : 487a-da52-d4f0
MAC address                             : 000b-c002-5e39
VLAN                                    : 1
Authentication method                   : Certificate
Current state                           : Online
    Authentication state                : Authenticated
    Unicast key negotiation state       : Established
    Multicast key negotiation state     : Established
    Authorization state                 : Idle
    Accounting state                    : Success
Uptime                                  : 00:02:26

AP name                                 : ap1
Radio ID                                : 1
SSID                                    : wapi1
BSSID                                   : 487a-da52-d4f0
MAC address                             : 000b-c002-5e2f
VLAN                                    : 1
Authentication method                   : Certificate
Current state                           : Online
    Authentication state                : Authenticated
    Unicast key negotiation state       : Established
    Multicast key negotiation state     : Established
    Authorization state                 : Idle
    Accounting state                    : Success
Uptime                                  : 00:02:30
```

1.13 常见配置错误举例

1.13.1 Client 上线失败

1. 故障现象

AP 关联到 AC 之后，Client 关联 AP 失败。在 AC 上通过 **`display wapi user`** 命令查看到没有 WAPI 用户存在或者其不处于 Online 状态，表明 Client 上线失败。

2. 故障分析

- Client 成功关联到 AP 的前提是 AP 已正确关联到 AC。
- 对于预共享密钥认证，须保证 Client 与 AP 的预共享密钥一致；对于标准证书鉴别，须保证 Client 与 AP 的证书正确。

3. 处理过程

(1) 检查 AP 是否已关联到 AC。在 AC 上使用 **display wlan ap all** 命令查看 AP 的状态是否为 Run。

(2) 检查 AP 和 Client 的配置是否正确：

- 当采用预共享密钥认证时，检查 Client 与 AP 的预共享密钥是否一致。在 AC 上通过 **display current-configuration** 命令查看 AP 的预共享密钥类型和预共享密钥值是否与 Client 的一致：对于预共享密钥类型，当 Client 为 ASCII 类型时，AP 必须为字符串类型；当 Client 为 HEX 类型时，AP 必须为十六进制数类型。
- 当采用标准证书认证时，检查 CA、AC 和 AS 的证书是否正确。在 AC 上通过 **display pki certificate** 命令查看各证书内容是否正确，特别要注意：若某证书的签名算法不是 ECDSA，则需先删除该证书所在 PKI 域内的所有证书，再将该域的证书签名算法配置为 ECDSA，然后重新安装该域内的所有证书。

1.13.2 计费异常

1. 故障现象

计费出现异常，如计费失败。

2. 故障分析

- 检查认证方案、计费方案、认证服务器、计费服务器的配置是否正确。
- 检查计费服务器是否可达。

3. 处理过程

- 如果 WAPI 证书认证方式为标准方式，则计费方案可以采用 None 方案，也可以采用 RADIUS 方案（计费服务器不能使用 iMC）。
- 必须使用 **wapi domain** 命令用来指定 WAPI 认证所属的 ISP 域。
- 保证计费服务器可达。

1.13.3 用户上线后无法 ping 通

1. 故障现象

用户上线后，客户端无法 ping 通 AC 或其它设备。

2. 故障分析

如果使用 AC 进行加解密，检查 AC 的内存是否大于等于 1G。

由于无线网卡可能不支持 QoS，AC 默认开启 WMM 功能，这种情况下可能会导致报文不通。

3. 处理过程

如果 AC 的内存小于 1G，请使用内存大于等于 1G 的 AC 或者在现有 AC 上增加内存。

在 Radio 视图下配置 **wmm disable** 命令。